The President's National Security Telecommunications Advisory Committee

R&D Exchange
Cyber/Software Breakout Session 2

Carl Landwehr, National Science Foundation
Sami Saydjari, Cyber Defense Agency

March 14, 2003

What we did

- **What we did:**
  - **Scoping discussion**
  - **Desired end states**
  - **Research topics driving to the end states**
  - **Final recommendations/actions**

Research Areas and Assessment

Research Topic	Decision	System	E&T	Bldg Blocks	Policy	Difficulty	Time Range	Pay-off
Security Metrics. For example, create benchmarking (automated testing/validation) systems publicly available, perhaps as element of certification. Must define trustworthiness from arch/software persective	p	s				H	M	H
Graded Adversary Threat Models	p	s			s	M	S	M
Figure out where we are most vulnerable; Case studies for threat assessment: scenario development and testing (e.g. of “nightmare” scenario). Purpose to validate national vulnerability assessment, eg	p	s				M	S	H
Define criticality, criteria, and tiered criticality model.	p	s				M	M	M
Management Science of security aspects (ROI and risk). Determining cost to industry of security features/assurance (in $, time to market, performance, etc.). Cost-effective techniques for achieving (validatable) trustworthy systems	p	s				M	M	H
Research in tradeoffs between edge security and internal network security.	p	s				M	S	M
Explore develop of national cybersecurity testbed. Simulation mode, to assess attack effects, support training.	p	s				M	M	H
Systematic study of application of different exisiting telecomm systems for NS/EP application. We have choices today, but perhaps haven’t capitalized on them.	p	s				L	S	M
Research in economic models for software vulnerability detection/removal.	p	s			s	M	S	H

Cyber/Software: Current State of Trustworthiness

- **NS/EP networks have operated reasonably well in practice in many situations of naturally induced faults, errors and failures, including physical attacks.**
- **Economic conditions can trigger changes in the trustworthiness of the underlying telecommunications and computing fabric of NS/EP systems.**
- **NS/EP managers charged with acquiring and managing network resources often face difficult choices among alternatives and lack a strong rational basis for making decisions affecting system trustworthiness.**
- **Reports of new vulnerabilities in NS/EP networks are dealt with largely through intensive manual response.**
- **NS/EP networks and components are significantly vulnerable to malicious attacks exploiting naturally occurring faults and errors.**
- **NS/EP networks would be significantly vulnerable to sophisticated attacks aiming to insert vulnerabilities or sabotage data integrity.**
- **NS/EP network managers can respond to reports of vulnerabilities and incidents with substantial manual coordination in a period of hours to weeks.**

Cyber/Software: Technology To Improve Trustworthiness

- **Develop a Rational Basis for Information Assurance decision making**
- **Improve Systems Understanding and Control**
- **Develop a Well Trained Workforce for Research and Operation**
- **Improve Trustworthiness of Building Blocks**
  - **Better attribution**
  - **Better damage prevention and limitation**
- **Develop Policy fostering Cooperation, Collaboration, Prosecution**

Cyber/Software: Impediments to Future R&D on Trustworthiness

- **Lack of trained workforce of operators and researchers**
- **Lack of convincing case for R&D funding, failing widespread disaster**
- **Lack of a clearinghouse for information on relevant R&D programs**
- **Difficulty of gaining the benefit of the R&D products (not an impediment to R&D per se, but impediment to achieving more trustworthy systems)**
- **Outsourcing of software/hardware, especially offshore**
- **Inadequate, outdated, non-uniform critical infrastructure standards for minimum security in procurements**

Cyber/Software: Input to the OSTP and the NSTAC

- **Caution regarding potential unintended consequences from achieving some research goals**
  - **Individuals and research projects by nature focus on the problem at hand**
  - **Results that could be beneficial sometimes are lost because of external factors not taken into account**
  - **Need for discussion of potential uses of research to proceed in parallel with the research**
- **Recommend longer term examination of research topic areas by a professionally diverse group such as this one**
  - **Possible continuing involvement via electronic means**
  - **Focus on breakthrough technologies**

Cyber/Software: Agenda for Action

- **Set a national vision for trustworthiness of NS/EP systems**
- **Develop scientifically validated, compelling "national security" case (e.g. simulate scenarios) for the vulnerability of existing NS/EP systems**
- **Advocate to the White House research to realize the vision**
  - **Funding**
  - **Coordination: government and industry**